UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/074,411	02/12/2002	Roger Eastvold	390P010777-US (PAR)	7013

7590 03/29/2007

Geza C. Ziegler, Jr.
PERMAN & GREEN, LLP
425 Post Road
Fairfield, CT 06430

EXAMINER	
PATEL, ASHOKKUMAR B	
ART UNIT	**PAPER NUMBER**
2154	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/29/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/074,411	EASTVOLD, ROGER	
	Examiner	Art Unit	
	Ashok B. Patel	2154	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 December 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-36 are subject to examination.

Response to Arguments

2. Applicant's arguments filed 12/18/2006 have been fully considered but they are not persuasive for the following reasons:

Applicant's response to 35 U.S.C. 112, first paragraph rejection:

"Claims 1, 6, and 11 are definite under 35 U.S.C. 112, first paragraph. One example of the different data" recited in claims 1, 6, and 11 is the **"authentication dialog box"** disclosed in the specification at page 14, line 26 through page 15, line 2."

Examiner's response:

Please also note that "It is the claims that define the claimed invention, and it is claims, not specifications that are anticipated or unpatentable. *Constant v. Advanced Micro-Devices Inc.*, 7 USPQ2d 1064."

As such the following previous rejection under 35 U.S.C. 112, first paragraph, is maintained.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 1-36 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter

which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Referring to claim 1,

As pointed out previously, the phrase " send a different data" to the local network, is not described in the specification, the Applicant was requested to cancel the new matter in the reply to the previous Office Action.

Even if the above new matter is considered to be "a not new matter", claim 1 recites in the preamble " A system for accessing data remotely from a network, comprising:" and the module is configured to receive and process a first data from the remote network and send a different data to the local network based on the first data received from the remote network", **how is it possible** to send ""**authentication dialog box", as a different data as a response to the request for an access in the wrong direction, that is being** "send a different data to the local network based on the first data received from the remote network."

Referring to claims 2-5, 33 and 35,

Claims 2-5 are rejected because of their dependency on the rejected claim 1.

Referring to claim 6,

As pointed out previously, the phrase " send a different data" to the local network, is not described in the specification, the Applicant was requested to cancel the new matter in the reply to the previous Office Action.

Even if the above new matter is considered to be "a not new matter", claim 1 recites in the preamble " A system for accessing a local network from a remote network through an intermediate network, comprising:" and "the module being configured to receive and process data from at least one of the plurality of users of the remote network and send a different data to at least one of the plurality of equipment of the local network based on the data received from the remote network", **how is it possible** to send ""**"authentication dialog box", as a different data as a response to the request for an access in the wrong direction, that is being** "the module being configured to receive and process data from at least one of the plurality of users of the remote network and send a different data to at least one of the plurality of equipment of the local network based on the data received from the remote network."

Referring to claims 7-10 and 34,

Claims 7-10 are rejected because of their dependency on the rejected claim 6.

Referring to claim 11,

As pointed out previously, the phrase " send a different data" to the local network, is not described in the specification, the Applicant was requested to cancel the new matter in the reply to the previous Office Action.

Even if the above new matter is considered to be "a not new matter", claim 1 recites in the preamble " A data system comprising:" and "wherein the intermediate network is configured to selectively receive and selectively process data from the remote network depending on a set of predetermined criteria applied by the intermediate network and send a different data to the local network", **how is it possible**

to send ""**authentication dialog box", as a different data as a response to the request for an access in the wrong direction, that is being** "send a different data to the local network .."

Referring to claims 12-23 and 36,

Claims 7-10 are rejected because of their dependency on the rejected claim 6.

For the reasons stated above, the previous rejection is maintained without considering the claim amendments.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless-

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 1, 2, 4-7, 9-13, 15-23 are rejected under 35 U.S.C. 102(e) as being anticipated by Crist et al. (hereinafter Crist) (US 6, 879, 940 B1)

Referring to claim 1,

Crist teaches a system for accessing data remotely from a network, comprising:

a local network interface permitting data transfer (Fig. 3, element 36, "Host Network", col. 7, line 8-10, "Additionally, the particular client may only connect to their local workstation 32 after being screened by the host's security system.") between a local network (Fig. 3, elements 34, 11) and an intermediate network (Fig. 3, elements

32, col. 7, line 12-17, "The host schedules particular times on the test system 34 for particular single clients, who may then operate the test system 34 as described in the first embodiment. A switch matrix 33, is provided so that a host network 36 may connect or disconnect from the test system 34 as described in the previous embodiment.");

a remote network interface device (Fig. 3, element 30, "Remote Workstation", col. 5, line 7-33) permitting data transfer between the intermediate network (Fig. 3, elements 32, col. 7, line 12-17), and a remote network (col. 5, line 7-33); and

a module located within the intermediate network through which all data transferring between the local network and the remote network must pass, the module being configured to receive and process data from the remote network and send a different data to the local network based on the data received from the remote network. (col. 6, line 1-3, "The test program must at some point in time be transferred to the local workstation 7 in order to run the test system 8 from the local workstation 7. In this embodiment, the test system 8 is connected to the host's network 10 (LAN). The local workstation 7 is desirable because of the large quantity of data that must be transferred to and from the test system 8.")

Referring to claim 2,

Crist teaches the system of claim 1, wherein the data transfer between each of the networks occurs via the Internet Protocol (IP), and wherein each network has its own unique IP address. (col. 5, line 7-33)

Referring to claim 4,

Crist teaches the system of claim 1, wherein the module exchanges data with an equipment diagnostic monitor system located within the intermediate network, and wherein the equipment diagnostic monitor system has the function of monitoring tests performed on at least one tool residing within the local network (col. 6, line 1-3, "The test program must at some point in time be transferred to the local workstation 7 in order to run the test system 8 from the local workstation 7. In this embodiment, the test system 8 is connected to the host's network 10 (LAN). The local workstation 7 is desirable because of the large quantity of data that must be transferred to and from the test system 8.").

Referring to claim 5,

Crist teaches the system of claim 4, wherein the equipment diagnostic monitor system collects and analyzes data from tests performed on the at least tool. (col. 6, line 1-3, "The test program must at some point in time be transferred to the local workstation 7 in order to run the test system 8 from the local workstation 7. In this embodiment, the test system 8 is connected to the host's network 10 (LAN). The local workstation 7 is desirable because of the large quantity of data that must be transferred to and from the test system 8.", col. 4, line 15-21).

Referring to claim 6,

Crist teaches a system for accessing a local network from a remote network through an intermediate network , comprising:

a local network interface permitting data transfer (Fig. 3, element 36, "Host Network", col. 7, line 8-10, "Additionally, the particular client may only connect to their

local workstation 32 after being screened by the host's security system.") between a local network (Fig. 3, elements 34, 11) and the intermediate network (Fig. 3, elements 32, col. 7, line 12-17, "The host schedules particular times on the test system 34 for particular single clients, who may then operate the test system 34 as described in the first embodiment. A switch matrix 33, is provided so that a host network 36 may connect or disconnect from the test system 34 as described in the previous embodiment.");

a remote network interface device (Fig. 3, element 30, "Remote Workstation", col. 5, line 7-33) permitting data transfer between the remote network (Fig. 3, elements 32, col. 7, line 12-17), and the intermediate network (col. 5, line 7-33);

a module located within the intermediate network, the module being configured to receive and process data from the remote network and send a different data to the local network based on the data received from the remote network (col. 6, line 1-3, "The test program must at some point in time be transferred to the local workstation 7 in order to run the test system 8 from the local workstation 7. In this embodiment, the test system 8 is connected to the host's network 10 (LAN). The local workstation 7 is desirable because of the large quantity of data that must be transferred to and from the test system 8."); and

an equipment diagnostic monitor system for monitoring the health of equipment within the local network, the equipment diagnostic monitoring system being located within the intermediate network, wherein the equipment diagnostic monitor system monitors tests performed on at least one item residing within the local network (col. 6,

line 1-3, "The test program must at some point in time be transferred to the local workstation 7 in order to run the test system 8 from the local workstation 7. In this embodiment, the test system 8 is connected to the host's network 10 (LAN). The local workstation 7 is desirable because of the large quantity of data that must be transferred to and from the test system 8.")

Referring to claim 7,

Crist teaches the system of claim 6, wherein the data transfer between each of the networks occurs via the Internet Protocol (IP). (col. 5, line 7-33).

Referring to claim 9,

Crist teaches the system of claim 6, wherein the equipment diagnostic monitor system collects and analyzes data from the tests performed on the at least one item. (col. 6, line 1-3, col. 4, line 15-21)

Referring to claim 10,

Crist teaches the system of claim 6, wherein a user on the remote network may request that tests be performed on the at least one item, and may upload data to the remote network, from the tests performed on the at least one item. (Abstract)

Referring to claim 11,

Crist teaches a data system (Fig. 4), comprising:

a local network interface device (Fig. 3, element 36, "Host Network", col. 7, line 8-10, "Additionally, the particular client may only connect to their local workstation 32 after being screened by the host's security system.") enabling data transfer between a local network (Fig. 3, elements 34, 11) and an intermediate network ((Fig. 3, elements

32, col. 7, line 12-17, "The host schedules particular times on the test system 34 for particular single clients, who may then operate the test system 34 as described in the first embodiment. A switch matrix 33, is provided so that a host network 36 may connect or disconnect from the test system 34 as described in the previous embodiment.");

a remote network interface device (Fig. 3, element 30, col. 5, line7-33) enabling data transfer between a remote network (col. 5, line 7-33) and the intermediate network Fig. 3, element 32, col.7, line 12-17) ; and

an equipment diagnostic monitor system for monitoring the health of equipment within the local network, the equipment diagnostic monitoring system being located within the intermediate network, wherein the equipment diagnostic monitor system monitors tests performed on at least one item in the local network (col. 6, line 1-3, "The test program must at some point in time be transferred to the local workstation 7 in order to run the test system 8 from the local workstation 7. In this embodiment, the test system 8 is connected to the host's network 10 (LAN). The local workstation 7 is desirable because of the large quantity of data that must be transferred to and from the test system 8.")

wherein the intermediate network is configured to receive and selectively process data from the remote network depending on a set of predetermined criteria applied by the intermediate network and send a different data to the local network based on the selectively processed data.(col. 6, line 57 through col. 7, line 17).

Referring to claim 12,

Crist teaches the system of claim 11, further comprising a security module located within the intermediate network, through which all data transferring between the local network and the remote network must pass. (Fig. 3, element 33).

Referring to claim 13,

Crist teaches the system of claim 12, wherein data transfer between each of the networks occurs via the Internet Protocol (IP). (col. 5, line 7-33).

Referring to claim 15,

Crist teaches the system of claim 11, wherein the equipment diagnostic monitor system collects and analyzes data from tests performed on the at least one item. (col. 6, line 1-3, col. 4, line 15-21)

Referring to claim 16,

Crist teaches the system of claim 11, wherein the equipment diagnostic monitor system is configured to execute or ignore a request by a user on the remote network based on a set of predetermined criteria, wherein the user requests that tests be performed on the at least one item, and that data from previous tests performed on the at least one item be uploaded (col.6, line 38-47, col. 6, line 57 through col. 7, line 17).

Referring to claim 17,

Crist teaches the system of claim 11, wherein a user on the remote network sends a suggestion regarding the operation of the at least one item being monitored to an entity managing the item on the local network. (col. 6, line14-38)

Referring to claim 18,

Crist teaches the system of claim 11, wherein the equipment diagnostic monitor system sends an alert to a predetermined entity when the analysis of tool data indicates that the at least one item is operating outside of a predetermined performance range. (col. 4, line 15-21)

Referring to claim 19,

Crist teaches the system of claim 1 further comprising a remote control proxy server in the intermediate network that is between the local network and the remote network that prevents direct IP routing to a device in the local network that is being accessed by the remote network.(Fig. 3, element 36)

Referring to claims 20, 21 and 22,

Crist teaches the system of claim further comprising a semiconductor tool coupled to the local network, a user being able to access the semiconductor tool via the remote network, and the system of claim 20, wherein the intermediate network further comprises an equipment diagnostic monitor system that monitors and analyzes the semiconductor tool, and the system of claim 21, wherein the equipment diagnostic monitor system controls tests performed by software within the semiconductor tool, saves data from the tests and sends out alerts to a remote user via the remote network when the semiconductor tool is operating outside a predetermined performance range. (col.4, line15-21, col. 6, line 1-3, col. 6, line 57 through col. 7, line 17)

Referring to claim 23,

Crist teaches the system of claim 21, wherein the equipment monitor system effects access to the semiconductor tool by a remote user. (col. 6, line 57 through col. 7, line 17)

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 3, 8 and 14 are rejected under 35 U.S.C. 103(a) as being Crist et al. (hereinafter Crist) (US 6, 879, 940 B1) in view of Reid et al. (hereinafter Reid)(US 6, 182, 226 B1)

Referring to claim 3,

Keeping in mine the teachings of Crist as stated above, Crist explicitly fails to teach the system of claim 2, wherein the module hides the IP addresses of the remote network and the local network from each other.

Reid teaches "A rewrite node is a point in an access rule where source or destination addresses are mapped to other source or destination addresses. Destination IP address rewrites allow an inbound connection through network address translation (NAT) address hiding to be remapped to a destination inside the NAT barrier. Source address rewrites can be used on outbound connections to make the source appear to be one of many external addresses. This process allows the internal hosts to

be aliased to external addresses. Rewrites can be based on any connection criteria, including users.", col. 6, lines 46-56. (wherein the data transfer between each of the networks occurs via the Internet Protocol (IP), and wherein each network has its own unique IP address, and the system of claim 2, wherein the module hides the IP addresses of the remote network and the local network from each other.)

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to add the teachings of the Reid to the firewalls of the service facility of Crist such that address rewrites for inbound and outbound can be implemented based on any connection criteria, including users.

It would have been obvious because it provides a method for controlling interactions between networks by the use of firewalls with defined regions as taught by Reid.

Referring to claim 8,

Keeping in mine the teachings of Crist as stated above, Crist explicitly fails to teach the system of claim 7, wherein the module hides the IP addresses of the local network and the remote network from each other.

Reid teaches "A rewrite node is a point in an access rule where source or destination addresses are mapped to other source or destination addresses. Destination IP address rewrites allow an inbound connection through network address translation (NAT) address hiding to be remapped to a destination inside the NAT barrier. Source address rewrites can be used on outbound connections to make the source appear to be one of many external addresses. This process allows the internal hosts to

be aliased to external addresses. Rewrites can be based on any connection criteria, including users.", col. 6, lines 46-56. (wherein the data transfer between each of the networks occurs via the Internet Protocol (IP), and wherein each network has its own unique IP address, and the system of claim 2, wherein the module hides the IP addresses of the remote network and the local network from each other.)

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to add the teachings of the Reid to the fire wall of the service facility of Crist such that address rewrites for inbound and outbound can be implemented based on any connection criteria, including users.

It would have been obvious because it provides a method for controlling interactions between networks by the use of firewalls with defined regions as taught by Reid.

Referring to claim 14,

Keeping in mine the teachings of Crist as stated above, Crist explicitly fails to teach the system of claim 13, wherein the module hides the IP addresses of the local network and the remote network from each other.

Reid teaches "A rewrite node is a point in an access rule where source or destination addresses are mapped to other source or destination addresses. Destination IP address rewrites allow an inbound connection through network address translation (NAT) address hiding to be remapped to a destination inside the NAT barrier. Source address rewrites can be used on outbound connections to make the source appear to be one of many external addresses. This process allows the internal hosts to

be aliased to external addresses. Rewrites can be based on any connection criteria, including users.", col. 6, lines 46-56. (wherein the data transfer between each of the networks occurs via the Internet Protocol (IP), and wherein each network has its own unique IP address, and the system of claim 2, wherein the module hides the IP addresses of the remote network and the local network from each other.)

Therefore, it would have been obvious to one having ordinary skill in the art at the time of invention was made to add the teachings of the Reid to the fire wall of the service facility of Crist such that address rewrites for inbound and outbound can be implemented based on any connection criteria, including users.

It would have been obvious because it provides a method for controlling interactions between networks by the use of firewalls with defined regions as taught by Reid.

9. Claims 24-32 are new claims for which the following rejections is provided.

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

11. Claims 24 and 28-32 are rejected under 35 U.S.C. 102(e) as being anticipated by Pasadyn et al. (hereinafter Pasadyn)(US 2005/0221514 A1)

Referring to claim 24,

Pasadyn teaches a data system for accessing remote equipment (Figs11-14), comprising:

a first network interface device (Figs. 13 and 14, element 1330, 1430) enabling data transfer between a local network (Figs. 13 and 14, elements 1310, 1305 shown by solid Arrow connected to element 130 and 1430) and an intermediate network (Figs. 13 and 14, Elements 1320, 1440, shown by solid Arrow connected to element 1330, 1430);

a second network interface device (Figs. 13 and 14, elements 1320 and 1440) enabling data transfer between a remote network ([0062] In various illustrative embodiments, the engineer may be provided with advanced process data monitoring capabilities, such as the ability to provide historical parametric data in a user-friendly format, as well as event logging, real-time graphical display of both current processing parameters and the processing parameters of the entire run, and remote, i.e., local site and worldwide, monitoring.", para.[0081], "The Advanced Process Control (APC) framework permits remote access and monitoring of the process performance.") and the intermediate network (Figs. 13 and 14, Elements 1320, 1440, shown by solid Arrow connected to element 1330, 1430); and

an equipment diagnostic monitor system for monitoring a health of the equipment ([0067] Turning to FIG. 12, in this particular embodiment, the processing process characteristic parameters are measured and/or monitored by tool sensors (not shown). The outputs of these tool sensors are transmitted to a computer system 1230 over a line

1220. The computer system 1230 analyzes these sensor outputs to identify the characteristic parameters."), the equipment being located in the local network (Fig. 12, 13 and 14, elements 1210, 1205, 1310, 1305, 1410), the equipment diagnostic monitoring system being located within the intermediate network (para. [0107], "Returning again to FIG. 15, the calculation of new settings comprises, as set forth in box 1530, modeling the characteristic parameter(s) using an adaptive sampling processing model. This modeling may be performed by the Matlab.RTM. plug-in. In this particular embodiment, only known, potential characteristic parameters are modeled and the models are stored in a database 1335 accessed by a machine interface 1430. The database 1335 may reside on the workstation 1330, as shown, or some other part of the Advanced Process Control (APC) framework. For instance, the models might be stored in the data store 1360 managed by the Advanced Process Control (APC) system manager 1440 in alternative embodiments. The model will generally be a mathematical model, i.e., an equation describing how the change(s) in processing recipe control(s) affects the processing performance, and the like. The models described in various illustrative embodiments given above, and described more fully below, are examples of such models."), the equipment diagnostic monitoring system having at least a monitoring module, an analysis module (para. [0067],"Turning to FIG. 12, in this particular embodiment, the processing process characteristic parameters are measured and/or monitored by tool sensors (not shown). The outputs of these tool sensors are transmitted to a computer system 1230 over a line 1220. The computer system 1230 analyzes these sensor outputs to identify the characteristic parameters."), an alerts

module (para.[0059], "The adaptive sampling processing modeling of the monitored sensor data 115 in the adaptive sampling processing modeling with model predictive control (MPC) or proportional-integral-derivative (PID) tuning step 130, may be used to alert an engineer of the need to adjust the processing performed in any of a variety of processing steps, such as the processing tool 105 and/or the other processing steps 140.") and an active transfer module (para. [0067],"Turning to FIG. 12, in this particular embodiment, the processing process characteristic parameters are measured and/or monitored by tool sensors (not shown). The outputs of these tool sensors are transmitted to a computer system 1230 over a line 1220. The computer system 1230 analyzes these sensor outputs to identify the characteristic parameters.");

wherein the equipment diagnostic monitor system is configured to monitor at least one activity performed on the equipment in the local network (para. [0069], "In the embodiment of FIG. 12, a database 1235 stores a plurality of models that might potentially be applied, depending upon which characteristic parameter is measured. This particular embodiment, therefore, requires some a priori knowledge of the characteristic parameters that might be measured. The computer system 1230 then extracts an appropriate model from the database 1235 of potential models to apply to the measured characteristic parameters. If the database 1235 does not include a.sub.1 appropriate model, then the characteristic parameter may be ignored, or the computer system 1230 may attempt to develop one, if so programmed. The database 1235 may be stored on any kind of computer-readable, program storage medium, such as an optical disk 1240, a floppy disk 1245, or a hard disk drive (not shown) of the computer

system 1230. The database 1235 may also be stored on a separate computer system (not shown) that interfaces with the computer system 1230.")and the intermediate network is configured to receive and selectively process data from the remote network depending on a set of predetermined criteria applied by the intermediate network and send the processed data to the local network (para. [0079], "Referring now to both FIGS. 13 and 14, the processing tool 1310 communicates with a manufacturing framework comprising a network of processing modules. One such module is an Advanced Process Control (APC) system manager 1440 resident on the computer 1340. This network of processing modules constitutes the Advanced Process Control (APC) system. The processing tool 1310 generally comprises an equipment interface 1410 and a sensor interface 1415. A machine interface 1430 resides on the workstation 1330. The machine interface 1430 bridges the gap between the Advanced Process Control (APC) framework, e.g., the Advanced Process Control (APC) system manager 1440, and the equipment interface 1410. Thus, the machine interface 1430 interfaces the processing tool 1310 with the Advanced Process Control (APC) framework and supports machine setup, activation, monitoring, and data collection. The sensor interface 1415 provides the appropriate interface environment to communicate with external sensors such as LabView.RTM. or other sensor bus-based data acquisition software. Both the machine interface 1430 and the sensor interface 1415 use a set of functionalities (such as a communication standard) to collect data to be used. The equipment interface 1410 and the sensor interface 1415 communicate over the line 1320 with the machine interface 1430 resident on the workstation 1330.")

Referring to claim 28,

Pasadyn teaches the system of claim 24, wherein the equipment diagnostic monitor system is configured to collect and analyze data from at least one test performed on the equipment (para. [0067],"Turning to FIG. 12, in this particular embodiment, the processing process characteristic parameters are measured and/or monitored by tool sensors (not shown). The outputs of these tool sensors are transmitted to a computer system 1230 over a line 1220. The computer system 1230 analyzes these sensor outputs to identify the characteristic parameters.", para. [0324], "FIG. 25 contains the results of the test.").

Referring to claim 29,

Pasadyn teaches the system of claim 24, wherein the equipment diagnostic monitor system is configured to execute or ignore a request from the user on the remote network based on a set of predetermined criteria, wherein the user requests that tests be performed on the equipment, and that other data be uploaded from previous tests performed on the equipment. para. [0324], "FIG. 25 contains the results of the test.", (para. [0069], "In the embodiment of FIG. 12, a database 1235 stores a plurality of models that might potentially be applied, depending upon which characteristic parameter is measured. This particular embodiment, therefore, requires some a priori knowledge of the characteristic parameters that might be measured. The computer system 1230 then extracts an appropriate model from the database 1235 of potential models to apply to the measured characteristic parameters. If the database 1235 does

not include a.sub.1 appropriate model, then the characteristic parameter may be ignored, or the computer system 1230 may attempt to develop one, if so programmed. The database 1235 may be stored on any kind of computer-readable, program storage medium, such as an optical disk 1240, a floppy disk 1245, or a hard disk drive (not shown) of the computer system 1230. The database 1235 may also be stored on a separate computer system (not shown) that interfaces with the computer system 1230.", para. [0359] The process control server 3090 may initiate pre-processing and/or post-processing metrology events as necessary to determine the operating states of the tools 3030-3080. The data from the metrology events may be returned to the process control server 3090 (or some other computing resource on the network 3020) and analyzed. Alternatively, the process control server 3090 may access process data already collected and stored in the data store 30110. For example, pre-process and post-process metrology data may have been collected for various tools to generate statistical data for process control and/or fault detection.").

Referring to claim 30,

Pasadyn teaches the system of claim 24, wherein the local network is configured to receive and display a suggestion from the user on the remote network regarding the operation of the equipment being monitored on the local network (para. [0078], "When a process step in the processing tool 1310 is concluded, the semiconductor workpieces 1305 being processed in the processing tool 1310 are examined at a review station 1317. The review station 1317 need not be part of the processing tool 1310, but may, for example, be a separate tool and/or station.")

Referring to claim 31,

Pasadyn teaches the system of claim 24, wherein the equipment diagnostic monitor system is configured to send an alert to a predetermined entity when the analysis of the data indicates that the equipment is operating outside of a predetermined performance range ([0059] The adaptive sampling processing modeling of the monitored sensor data 115 in the adaptive sampling processing modeling with model predictive control (MPC) or proportional-integral-derivative (PID) tuning step 130, may be used to alert an engineer of the need to adjust the processing performed in any of a variety of processing steps, such as the processing tool 105 and/or the other processing steps 140. The engineer may also alter and/or adjust, for example, the setpoints for the processing performed in the processing tool 105, and/or the processing tool variable(s) and/or processing parameter(s) monitored and/or measured in the monitoring step 110.")

Referring to claim 32,

Pasadyn teaches the system of claim 24, further comprising an interface proxy located in the intermediate network, the interface proxy being configured to permit data transfer between the equipment diagnostic system and the remote network (para. [0081], "The Advanced Process Control (APC) framework permits remote access and monitoring of the process performance.", para. [0083], "There is also a script for the Advanced Process Control (APC) system manager 1440.")

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 25-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pasadyn et al. (hereinafter Pasadyn)(US 2005/0221514 A1) in view of Cunningham et al. (hereinafter Cunningham)(US 2002/0132607 A1).

Referring to claim 25-27,

Keeping in mind the teachings of Pasadyn as stated above, Pasadyn does not teach the system of claim 24, further comprising a security module located within the intermediate network, through which data transferred between the local network and the remote network passes, and the system of claim 25, wherein data transfer between each of the networks occurs via an Internet Protocol (IP), and the system of claim 26, wherein the security module hides an IP addresses of the local network and the remote network from each other.

Cunningham teaches at Fig. 2, element 34, 32 and 30, col. 6, line 1-48, "Referring now to FIG. 2, a first access control module 30 has been installed on the workstation 18 to enable the workstation to function as a passive access control station (PACS). A second instance of an access control module 32 is installed on the proxy server 28, so that this node functions as a proxy access control station (PRACS). Moreover, a third instance of an access control module 34 is installed on the firewall 16

in order to form a gateway access control station (GACS)(a security module located within the intermediate network, through which data transferred between the local network and the remote network passes.) A key point in the system and method is that the individual workstations 20 and 22 that are accessed by users can be managed without installing any software components specifically on those workstations. Network traffic is monitored and access to internal and external resources is controlled and managed either at choke points (represented by the proxy server 28 and the firewall 16) and/or non-intrusively at nodes which are not choke points (represented by the workstation 18). The access control modules 30, 32 and 34 can be installed, de-installed, and reinstalled on any of the nodes of the network at any time to suit potentially changing network topologies or changing access management policies. The location and configuration of each of the access control modules 30, 32 and 34 are selected by an installer based upon pragmatic factors in order to achieve a level of access control that is consistent with the access management policy. As previously noted, the first access control module 30 is not required, since the workstation 24 may serve the dual purpose of allowing a system operator to configure the rules base of access rules and non-intrusively monitoring traffic along the network. The second access control module 32 is optionally used in order to ensure that access is managed for all users who are accessing the WWW by configuring web browsers to operate via the proxy server 28. The third access control module 34 is optionally installed at the firewall 16 in order to validate that both the firewall and the other access control modules have indeed been configured correctly and are performing their desired duties.

Firewalls are sometimes difficult to configure, so organizations are increasingly adding second-line checks to their networks to ensure that absolute integrity is being maintained. However, the non-intrusive monitoring at the dedicated workstation 18 is capable of monitoring and controlling all access from all nodes on the network, regardless of TCP/IP protocol (wherein data transfer between each of the networks occurs via an Internet Protocol (IP)). This mechanism can be used to manage all network access that is not routed via the proxy server 28 with a high degree of probability that undesired access can indeed be blocked. Network traffic is non-intrusively monitored, but the system and method may be used to proactively block any requests for resources.", col. 7, line 11-14, "Other protocols are present and operational in TCP/IP networks and control operations such as routing and the translation of IP addresses to and from hostnames. A protocol referred to as ARP (Address Resolution Protocol) also maps IP addresses to Ethernet addresses (wherein the security module hides an IP addresses of the local network and the remote network from each other.)."

Cunningham's teachings would be so recognized by persons of ordinary skill, such that it would have been obvious for one in ordinary skill in the art at the time the invention was made to implement these teachings at the Pasadyn's APC System Manager such that when remotely accessed , Cunningham's module firewall as well as, as stated by Cunningham at col. 4, line 45-53 ," An advantage of the invention within a business environment is that the method and system protect employee productivity by ensuring that Internet access is used primarily for business purposes. Another advantage is that the bandwidth availability is used more efficiently. Access may be

dynamically controlled based upon factors such as the time of day and the day of the week. Another advantage is that internal security is enhanced by ensuring that access to internal computer resources is managed."

Conclusion

Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings of the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant in preparing responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ashok B. Patel whose telephone number is (571) 272-3972. The examiner can normally be reached on 6:30 am-4:30 pm.

NATHAN J. FLYNN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2800

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan A. Flynn can be reached on (571) 272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Abp
***